Attachment I

The following sample business associate agreement is provided for informational purposes only.

BUSINESS ASSOCIATE AGREEMENT

This Agreement is made effective Month day, year by and between the Wisconsin Department of Health Services, Name of Office, Division or Institution ("Covered Entity") and Name of Contractor/Business Associate ("Business Associate") collectively the "Parties").

1. BACKGROUND

This Agreement is specific to those services, activities, or functions performed by the Business Associate on behalf of the Covered Entity when such services, activities, or functions are covered by the Health Insurance Portability and Accountability Act of 1996 (HIPAA) including all pertinent regulations (45 CFR Parts 160 and 164) issued by the U.S. Department of Health and Human Services as either have been amended by Subtitle D of the Health Information Technology for Economic and Clinical Health Act (the "HITECH" Act), as Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (Pub. L. 111-5). Services, activities, or functions covered by this Agreement include, but are not limited to:

Insert description of covered services, activities for functions contracted for

The Covered Entity and Business Associate agree to modify the Contract to incorporate the terms of this Agreement and to comply with the requirements of HIPAA addressing confidentiality, security and the transmission of individually identifiable health information created, used or maintained by the Business Associate during the performance of the Contract and after Contract termination. The parties agree that any conflict between provisions of the Contract and the Agreement will by governed by the terms of the Agreement.

2. DEFINITIONS

The following terms shall have the following meaning in this Agreement. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms specified in the Privacy Rule.

a. "Breach" shall have the same meaning as the term "breach" in 45 CFR § 164.402 and shall include unauthorized acquisition, access, use or disclosure of Protected Health Information ("PHI") that compromises the security or privacy of such information.

b. "Corrective Action Plan" means a plan communicated by the Covered Entity to the Business Associate for the Business Associate to follow in the event of any threatened or actual use or disclosure of any PHI that is not specifically authorized by this Agreement, or in the event that any PHI is lost or cannot be accounted for by the Business Associate.

c. "Disclosure" means the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

d. "Electronic Health Record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

e. "Incident" means a use or disclosure of PHI by the Business Associate or subcontractor not authorized by this Agreement or in writing by the Covered Entity; a breach, a complaint by an individual who is the subject of any PHI created or maintained by the Business Associate on behalf of the Covered Entity; and any Federal HIPAA-related compliance contact. Also included in this definition is any attempted, successful or unsuccessful, unauthorized access, modification, or destruction of PHI, including electronic PHI, or interference with the operation of any information system that contains PHI.

f. "Individual" means the person who is the subject of Protected Health Information or the personal representative of an Individual as defined and provided for under applicable provisions of HIPAA.

g. "Protected Health Information (PHI)" means health information, including demographic information, created, received, maintained, or transmitted in any form or media by the Business Associate, on behalf of the Covered Entity, where such information relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the payment for the provision of health care to an individual, that identifies the individual or provides a reasonable basis to believe that it can be used to identify an individual.

h. "Unsecured Protected Health Information" means Protected Health Information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the HHS Secretary in guidance or as otherwise defined in the §13402(h) of the HITECH ACT and 45 CFR § 164.402.

i. Unless otherwise defined in this Agreement, terms used herein shall have the same meaning as those terms have in the Privacy Rule.

3. RESPONSIBILITIES OF BUSINESS ASSOCIATE

a. Business Associate shall not use or disclose any PHI except as permitted or required by the Contract or this Agreement, as permitted or required by law, or as otherwise authorized in writing by the Covered Entity, provided that such use or disclosure would not violate the HIPAA regulations if done by the Covered Entity.
b. Business Associate shall only use and disclose PHI if such use or disclosure complies with each applicable requirement of 45 CFR §164.504(e).
c. Business Associate shall be directly responsible for full compliance with relevant requirements of the Privacy Rule to the same extent as the Covered Entity.
d. Business Associate shall comply with Section 13405(b) of the HITECH Act when using, disclosing, or requesting PHI in relation to this Agreement by limiting disclosures as required by HIPAA.
e. Business Associate shall refrain from receiving any remuneration in exchange for any Individual's PHI unless (1) that exchange is pursuant to a valid authorization that includes a specification of whether PHI can be further exchanged for remuneration by the entity receiving PHI of that Individual, or (2) satisfies one of the exceptions enumerated in Section 13405(e)(2) of the HITECH Act or HIPAA regulations.
f. Business Associate shall refrain from marketing activities that would violate HIPAA, specifically Section 13406 of the HITECH Act.

4. SAFEGUARDING AND SECURITY OF PROTECTED HEALTH INFORMATION

a. Business Associate shall develop, implement, maintain, and use reasonable and appropriate administrative, technical, and physical safeguards that: (1) reasonably and appropriately safeguard the confidentiality, integrity, and availability of PHI, in any form of media, that it creates, receives, maintains, uses or transmits on behalf of the Covered Entity; and (2) to prevent use and disclosure of PHI other than as provided for by this Agreement.
b. Business Associate shall cooperate in good faith in response to any reasonable requests from the Covered Entity to discuss, review, inspect, and/or audit Business Associate's safeguards.

5. REPORTING OF INCIDENTS TO COVERED ENTITY BY BUSINESS ASSOCIATE

The Business Associate agrees to inform the Covered Entity of any Incident covered by this section, including an Incident reported to Business Associate by subcontractors or agents.

a. **Discovery of Incident**. The Business Associate must inform the Covered Entity by telephone call plus email or fax immediately within the same day of the discovery of any Incident, including but not limited to: the discovery of breach of security of PHI in computerized form if the PHI was, or is reasonably believed to be acquired by an unauthorized person; the discovery of any suspected security incident, intrusion or unauthorized use or disclosure of PHI in violation of this Agreement; or the discovery of potential loss of confidential data affecting this Agreement.

(i) The Incident shall be treated as "discovered" as of the first day on which the Incident is known to the Business Associate, or, by exercising reasonable diligence would have been known to the Business Associate.
(ii) Notification shall be provided to one of the contact persons as listed in section d.
(iii) Notification shall occur within the first business day that follows discovery of the Incident.

b. **Mitigation.** The Business Associate shall take immediate steps to mitigate any harmful effects of the unauthorized use, disclosure, or loss. The Business Associate shall reasonably cooperate with the Covered Entity's efforts to seek appropriate injunctive relief or otherwise prevent or curtail such threatened or actual breach, or to recover its PHI including complying with a reasonable Corrective Action Plan.

c. **Investigation of Breach**. The Business Associate shall immediately investigate the Incident and report in writing within one week to one of the contacts as listed in section 5d with the following information:
(i) Each Individual who's PHI has been or is reasonably to have been accessed, acquired, or disclosed during the Incident,
(ii) A description of the types of PHI that were involved in the Incident (such as full name, social security number, date of birth home address, account number and etc.).
(iii) A description of unauthorized persons known or reasonably believed to have improperly used or disclosed PHI or confidential data,
(iv) A description of where the PHI or confidential data is believed to have been improperly transmitted, sent, or utilized,
(v) A description of probable causes of the improper use or disclosure,
(vi) A brief description of what the Business Associate is doing to investigate the Incident, to mitigate losses and to protect against further Incidents,
(vii) The actions the Business Associate has undertaken or will undertake to mitigate any harmful effect of the occurrence, and
(viii) A corrective action plan that includes the steps the Business Associate has taken or shall take to prevent future similar Incidents.

d. **Covered Entity Contact Information.** To direct communications to above referenced Covered Entity's staff, the Business Associate shall initiate contact as indicated herein. The Covered Entity reserves the right to make changes to the contact information by giving written notice to the Business Associate.

Covered Entity Program Manager – Name & phone number	DHS Privacy Officer c/o Office of Legal Counsel Department of Health Services 1 W. Wilson St. Madison, WI 53707 608-266-5484	DHS Security Officer Department of Health Services 1 W. Wilson St. Madison, WI 53707 608-261-8310

6. RED FLAG RULES

The Business Associate shall be responsible for the implementation of an "Identity Theft Monitoring Policy and Procedure" to protect patient information that may be breached by the Business Associate if the Covered Entity is subject to the Federal Trade Commission Regulations Red Flag Rules which implements Section 114 of the Fair and Accurate Credit Transaction Act of 2003 16 C.F.R. § 681.2.

7. USE OR DISCLOSURE OF PROTECTED HEALTH INFORMATION BY SUBCONTRACTORS AND AGENTS OF THE BUSINESS ASSOCIATE

The Business Associate agrees to ensure that any agents or subcontractors, to whom the Business Associate provides PHI received from, or created or received by the Business Associate on behalf of the Covered Entity, agrees to the same restrictions and conditions in writing applicable to the Business Associate in this Agreement. The Business Associate shall ensure that any agent, including a subcontractor to whom a

Business Associate provides such information agrees to implement reasonable and appropriate safeguards to protect data; and report to the Covered Entity any Incident of which it becomes aware.

8. COMPLIANCE WITH ELECTRONIC TRANSACTIONS AND CODE SET STANDARDS

If the Business Associate conducts any Standard Transaction for, or on behalf, of a Covered Entity, the Business Associate shall comply, and shall require any subcontractor or agent conducting such Standard Transaction to comply, with each applicable requirement of Title 45, Part 162 of the Code of Federal Regulation. The Business Associate shall not enter into, or permit its subcontractors or agents to enter into, any Agreement in connection with the conduct of Standard Transactions for or on behalf of Covered Entity that:

a. Changes the definition, Health Information condition, or use of a Health Information element or segment in a Standard;
b. Adds any Health Information elements or segments to the maximum defined Health Information Set;
c. Uses any code or Health Information elements that are either marked "not used" in the Standard's Implementation Specification(s) or are not in the Standard's Implementation Specifications(s);
d. Changes the meaning or intent of the Standard's Implementations Specification(s).

9. ACCESS TO PROTECTED HEALTH INFORMATION

At the direction of the Covered Entity, the Business Associate agrees to provide access in accordance to 45 CFR 164.524 and Section 13405(f) of the HITECH Act to any PHI held by the Business Associate, which Covered Entity has determined to be part of Covered Entity's Designated Record Set, in the time and manner designated by the Covered Entity. This access will be provided to Covered Entity or, as directed by Covered Entity, to an Individual, in order to meet requirements under the Privacy Rule.

10. AMENDMENT OR CORRECTION TO PROTECTED HEALTH INFORMATION

At the direction of the Covered Entity, the Business Associate agrees to amend or correct PHI held by the Business Associate which the Covered Entity has determined is part of the Covered Entity's Designated Record Set, in the time and manner designated by the Covered Entity in accordance with 45 CFR 164.526.

11. DOCUMENTATION OF DISCLOSURES OF PROTECTED HEALTH INFORMATION BY THE BUSINESS ASSOCIATE

The Business Associate agrees to document and make available to the Covered Entity or (at the direction of the Covered Entity) to an Individual such disclosures of PHI to respond to a proper request by the Individual for an accounting of disclosures of PHI, in accordance with 45 CFR 164.528 and §13405(c) of the HITECH Act.

12. INTERNAL PRACTICES

The Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI available to the Covered Entity, or to the federal Secretary of Health and Human Services (HHS) in a time and manner determined by the Covered Entity or the HHS Secretary or designee, for purposes of determining compliance with the requirements of HIPAA. Further, the Business Associate agrees to promptly notify the Covered Entity of communications with HHS regarding PHI and will provide the Covered Entity with copies of any PHI or other information the Business Associate has made available to HHS under this provision.

13. TERM AND TERMINATION OF AGREEMENT

a. The Business Associate agrees that if in good faith the Covered Entity determines that the Business Associate has materially breached any of its obligations under this Agreement, the Covered Entity may:
   (i) Exercise any of its rights to reports, access and inspection under this Agreement;
   (ii) Require the Business Associate with a 30 day period to cure the breach or end the violation;

(iii) Terminate this Agreement if the Business Associate does not cure the breach or end the violation within the time specified by the Covered Entity;
(iv) Immediately terminate this Agreement if the Business Associate has breached a material term of this Agreement and cure is not possible; or
(v) If neither cure nor termination is feasible, report the violation to the Secretary of the U.S. Department of Health and Human Services.

b. Before exercising either (ii) or (iii), the Covered Entity will provide written notice of preliminary determination to the Business Associate describing the violation and the action the Covered Entity intends to take.

14. RETURN OR DESTRUCTION OF PROTECTED HEALTH INFORMATION

Upon termination, cancellation, expiration or other conclusion of this Agreement, the Business Associate will:

a. Return to the Covered Entity or, if return is not feasible, destroy all PHI and any compilation of PHI in any media or form. The Business Associate agrees to ensure that this provision also applies to PHI of the Covered Entity in possession of subcontractors and agents of the Business Associate. The Business Associate agrees that any original record or copy of PHI in any media is included in and covered by this provision, as well as all original or copies of PHI provided to subcontractors or agents of the Business Associate. The Business Associate agrees to complete the return or destruction as promptly as possible, but not more than **thirty (30)** business days after the conclusion of this Agreement. The Business Associate will provide written documentation evidencing that return or destruction of all PHI has been completed.

b. If the Business Associate destroys PHI, it shall be done with the use of technology or methodology that renders the PHI unusable, unreadable, or undecipherable to unauthorized individuals as specified by HHS in HHS guidance. Acceptable methods for destroying PHI include:
(i) Paper, film, or other hard copy media: shredded or destroyed in order that PHI cannot be read or reconstructed; and
(ii) Electronic media: cleared, purged or destroyed consistent with the standards of the National Institute of Standards and Technology (NIST).
Redaction is specifically excluded as a method of destruction of PHI, unless the information is properly redacted so as to be fully de-identified.

c. If the Business Associate believes that the return or destruction of PHI is not feasible, the Business Associate shall provide written notification of the conditions that make return or destruction not feasible. If the Business Associate and Covered Entity agree that return or destruction of PHI is not feasible, the Business Associate shall extend the protections of this Agreement to PHI and prohibit further uses or disclosures of the PHI of the Covered Entity without the express written authorization of the Covered Entity. Subsequent use or disclosure of any PHI subject to this provision will be limited to the use or disclosure that makes return or destruction not feasible.

15. COMPLIANCE WITH STATE LAW

a. The Business Associate acknowledges that PHI from the Covered Entity may be subject to state confidentiality laws. Business Associate shall comply with the more restrictive protection requirements between state and federal law for the protection of PHI.

16. MISCELLANEOUS PROVISIONS

a. Indemnification for Breach Notification. Business Associate shall indemnify the Covered Entity for costs associated with any Incident involving the acquisition, access, use or disclosure of Unsecured Protected Health Information in a manner not permitted under 45 C.F.R. part E.
b. Automatic Amendment. This Agreement shall automatically incorporate any change or modification of applicable state or federal law as of the effective date of the change or modification. The Business Associate agrees to maintain compliance with all changes or modifications to applicable state or federal law.

c. Interpretation of Terms or Conditions of Agreement. Any ambiguity in this Agreement shall be construed and resolved in favor of a meaning that permits the Covered Entity and Business Associate to comply with applicable state and federal law.

d. Survival. All terms of this Agreement that by their language or nature would survive the termination or other conclusion of this Agreement shall survive.

IN WITNESS WHEREOF, the undersigned have caused this Agreement to be duly executed by their respective representatives.

COVERED ENTITY	**BUSINESS ASSOCIATE**
By: _____	**By:** _____
Title: _____	**Title:** _____
Date: _____	**Date:** _____